National Infrastructure Protection Center CyberNotes

Issue #2001-13 *July 2, 2001*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between June 13 and June 28, 2001. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apple[1]	MacOS 8.0, 8.1, 9.0, 9.1	Personal Web Sharing 1.1, 1.5, 1.5.5	A remote Denial of Service vulnerability exists if a user has file sharing configured to authenticate personal web sharing logins.	No workaround or patch available at time of publishing.	MacOS Personal Web Sharing Authentication Denial of Service	Low	Bug discussed in newsgroups and websites.
Apple[2]	MacOS X 10.0, 10.0.1, 10.0.2, 10.0.3, 10.0.4	MacOS X 10.0-10.0.4	A vulnerability exists due to a misconfiguration of file permissions, which could let a malicious user gain sensitive information. (Vulnerability seems to affect users who installed system over earlier "Public Beta.")	No workaround or patch available at time of publishing.	MacOS X Insecure Default Permissions	Medium	Bug discussed in newsgroups and websites.

[1] Bugtraq, June 28, 2001.

[2] Bugtraq, June 26, 2001.

Vendor	**Operating System**	**Software Name**	**Vulnerability/ Impact**	**Patches/Workarounds/ Alerts**	**Common Name**	**Risk***	**Attacks/ Scripts**
Arcadia, Inc.[3]	Windows NT 4.0/2000	IC:Arcadia Internet Store 1.0	Multiple vulnerabilities exist in 'trradecli.dll': a remote Denial of Service vulnerability; a show path vulnerability; and an arbitrary file disclosure vulnerability, which could let a malicious user gain sensitive information.	No workaround or patch available at time of publishing.	IC:Arcadia Internet Store Multiple Vulnerabilities	Low/ Medium	Bug discussed in newsgroups and websites. Exploits and script have been published.
Atmel[4]	Multiple	Firmware 1.3	A vulnerability exists in the authentication mechanism of the Atmel VNET-B Simple Network Management Protocol (SNMP), which could let a remote malicious user gain sensitive information or gain access to or control a wireless LAN (WLAN).	Upgrade available at: **Linksys upgrade WAP11 1.4:** http://www.linksys.com/download/firmware.asp **Netgear upgrade ME102:** http://www.netgear.com/customer_services.asp	Atmel SNMP Community String	Medium/ **High**	Bug discussed in newsgroups and websites. Exploit has been published.
Caldera[5]	Unix	UnixWare 7	A buffer overflow vulnerability exists in the 'su' binary, which could let a malicious user execute arbitrary code as root.	Update available at: ftp://ftp.sco.com/pub/security/unixware/sr847407/erg711713a.Z	UnixWare 'su' Command Line Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Caldera[6]	Unix	UnixWare 7	A buffer overflow vulnerability exists in the 'cron' command, which could let a malicious user execute arbitrary code.	Update available at: ftp://ftp.sco.com/pub/security/unixware/sr847406/	UnixWare 'cron' Commandline Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Caldera[7]	Unix	UnixWare 7	A buffer overflow vulnerability exists in the uucp utilities, which could let a malicious user execute arbitrary code.	Update available at: ftp://ftp.sco.com/pub/security/unixware/sr847405/	UnixWare uucp Utilities Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Cisco Systems[8]	Multiple	IOS 11.3 & later	A vulnerability exists with the HTTP server component of Cisco IOS system software, which could let a remote malicious user gain full administrative privileges if local authentication databases are used.	For upgrade information see advisory located at: http://www.cisco.com/warp/public/707/IOS-httplevel-pub.html	Cisco IOS HTTP Configuration Arbitrary Administrative Access	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Cisco Systems[9]	Windows 95/98/NT 4.0	TFTP Server 1.1	A directory traversal vulnerability exists in the Cisco 6400 Access Concentrator Node Route Processor 2 (NRP2) module because Telnet access is allowed when no password is set, which could let a malicious user gain sensitive information.	Upgrade available at: http://www.cisco.com	Cisco TFTPD Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[3] NERF gr0up security advisory #2, June 21, 2001.
[4] Internet Security Systems Security Advisory, ISS-083, June 20, 2001.
[5] Caldera International, Inc. Security Advisory, CSSA-2001-SCO.2, June 27, 2001.
[6] Caldera International, Inc. Security Advisory, CSSA-2001-SCO.3, June 27, 2001.
[7] Caldera International, Inc. Security Advisory, CSSA-2001-SCO.4, June 27, 2001.
[8] Cisco Security Advisory, June 27, 2001.
[9] Sentry Research Labs , ID0201061701, June 18, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
DC Scripts[10]	Multiple	DCShop 1.002 beta	A vulnerability exists in the beta version of this product, which could allow a remote malicious user to request and obtain files containing confidential order data, including credit card and other private customer information, as well as the DCShop administrator login ID and password.	The vendor has issued an advisory which makes a number of recommendations addressing this issue; it is available at: http://www.dcscripts.com/dcforum/dcshop/44.html	DCShop File Disclosure	Medium	Bug discussed in newsgroups and websites. Exploits have been published.
Debian[11]	Unix	rxvt 2.6.2	A buffer overflow vulnerability exists in the tt_printf() function, which could let a malicious user execute arbitrary code/commands.	Update available at: http://security.debian.org/dists/stable/updates/main/	Rxvt Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
eXtremail[12]	Unix	eXtremail 1.0-1.1.9	A format string vulnerability exists in the 'flog()' function, which could let a remote malicious user gain root access.	Patch available at: http://www.extremail.com	eXtremail Remote Format String	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Gaztek[13]	Unix	ghttp 1.4	A buffer vulnerability exists, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Gaztek HTTP Daemon Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
GNU[14]	Multiple	Gnatsweb 2.7 beta, 2.8, 2.8.1, 3.95 GNATS 4	A vulnerability exists in the help system, which could let a remote malicious user gain sensitive information.	Patch available at: http://sources.redhat.com/gnats/gnatsweb/patches/	Gnatsweb Remote Command Execution	Medium	Bug discussed in newsgroups and websites. This vulnerability can be exploited with a Wweb browser.
Grant Averett[15]	Windows	Cerberus FTP Server 1.x	A buffer overflow vulnerability exists when a user is attempting to authenticate, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	No workaround or patch available at time of publishing.	Cerberus FTP Server Buffer Overflow Denial of Service	Low/**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
IBM[16]	Unix	AIX 4.3-4.3.3, 5.1	A vulnerability exists in a diagnostic reporting utility called 'diagrpt', which could let a malicious user gain root privileges.	Patch available at: ftp://aix.software.ibm.com/aix/efixes/security/diagrpt_efix.tar.Z	AIX diagrpt Arbitrary Privileged Program Execution	**High**	Bug discussed in newsgroups and websites. No exploit is required.

[10] DCScripts Advisory, June 13, 2001.
[11] Debian Security Advisory, DSA-062-1, June 16, 2001.
[12] Securiteam, June 28, 2001.
[13] Qitest1's Security Advisory #002, June 17, 2001.
[14] Gnatsweb Security Advisory, June 26, 2001.
[15] Cartel Advisory Code, CART-0101, June 21. 2001.
[16] IBM Global Services Managed Security Services, MSS-OAR-E01-2001:225.1, June 19, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Icecast[17]	Windows 2000, Unix	Icecast 1.3.7, 1.3.8 beta2, 1.310 Linux	Two security vulnerabilities exist: a remote Denial of Service vulnerability exists by adding an extra "/" or "\" after the requested mp3-file if the server has enabled the http-server file streaming support; and a directory traversal vulnerability exists because URL encoded characters are not filtered, which could let a remote malicious user view sensitive information.	No workaround or patch available at time of publishing.	Icecast Denial of Service and Directory Traversal	Low/ Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Internet Software Solutions[18]	Windows 98/98/ME/ NT 4.0/2000	Air Messenger LAN Server 3.4.2	Several vulnerabilities exist: a directory traversal vulnerability exists in the web interface; a path disclosure vulnerability exists when examining the webserver's http-header 'Location' field; and a vulnerability exists in the file 'pUser.Dat' because the username/password are stored in plaintext, which could let a remote malicious user gain sensitive information.	No workaround or patch available at time of publishing	AMLServer Directory Traversal, Path Disclosure, and Plaintext Storage	Medium	Bug discussed in newsgroups and websites. No exploit is required for the Directory Traversal and Plaintext Storage vulnerabilities. Exploit has been published for the Path Disclosure vulnerability.
Juergen Schoen-waelder[19]	Multiple	Scotty 2.1.10, 2.1.7, 2.1.8, 2.1.9	A buffer overflow vulnerability exists in 'ntping', which could let a malicious user execute arbitrary code.	Upgrade available at: ftp://ftp.ibr.cs.tu-bs.de/pub/local/tkined/scotty-2.1.11.tar.gz	Scotty 'ntping' Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Martin Schulze[20]	Unix	CFingerD 1.4.2, 1.4.3	Format string and buffer overflow vulnerabilities exist due to insufficient validation of input, which could let a malicious user gain elevated privileges. Successful exploitation of this vulnerability results in root access.	No workaround or patch available at time of publishing.	CFingerD Utilities Format String and Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Microburst[21]	Multiple	uDirectory 2.0	An input validation vulnerability exists, which could allow a remote malicious user to execute arbitrary commands.	No workaround or patch available at time of publishing.	uDirectory Remote Command Execution	**High**	Bug discussed in newsgroups and websites. Exploit script has been published

[17] Securiteam, June 28, 2001.
[18] Strumpf Noir Society Advisories, June 18, 2001.
[19] Securiteam, June 28, 2001.
[20] Bugtraq, June 21, 2001.
[21] Bugtraq, June 18, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[22]	Windows 2000	Windows 2000 SP1& SP2	A vulnerability exists due to improper permissions verification when submitting a password modify request, which could let a malicious user elevate their privileges. This is accomplished if LDAP requests are being made over a SSL session.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS01-036.asp	Microsoft Windows 2000 LDAP SSL Password Modification CVE Name: CAN-2001-0502	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[23]	Windows 2000	Word 97, 98, 2000, 2002, Word 98 & 2001 for Macintosh	A vulnerability exists because it is possible to modify a Word document in such a way as to prevent the security scanner from recognizing an embedded macro while still allowing it to execute, which could let a malicious user bypass the normal Word security.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS01-034.asp	Microsoft Malformed Word Document CVE Name: CAN-2001-0501	Medium	Bug discussed in newsgroups and websites.
Microsoft[24]	Windows NT 4.0/2000	Index Server 2.0; Indexing Services for Windows 2000; Indexing Service in Windows XP beta	An unchecked buffer vulnerability exists in 'idq.dll' ISAPI extension, which could let a malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS01-033.asp	Microsoft Index Server and Indexing Service ISAPI Extension Buffer Overflow CVE Name: CAN-2001-0500	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[25]	Windows NT 4.0/2000	IIS 4.0	A vulnerability exists in the way .asp requests are handled, which could let a malicious user gain sensitive information.	As a workaround convert the file system to NTFS. And consider removing reading access right for the IUSR_<hostname> from ASP scripts (only giving IUSR_<hostname> execute rights). In general follow: Microsoft's Security Best Practices: http://www.microsoft.com/technet/security/bestprac.asp or Internet Information Server 4.0 Security Checklist: http://www.microsoft.com/technet/security/iischk.asp or Secure Internet Information Services 5 Checklist: http://www.microsoft.com/technet/security/iis5chk.asp	Microsoft IIS Unicode .asp Source Code Disclosure	Medium	Bug discussed in newsgroups and websites.

[22] Microsoft Security Bulletin, MS01-036, June 25, 2001.
[23] Microsoft Security Bulletin, MS01-034, June 21, 2001.
[24] Microsoft Security Bulletin, MS01-033, June 18, 2001.
[25] VIGILANTE-Security Advisory, 2001001, June 22, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[26]	Windows NT 4.0/2000	Windows NT 4.0, SP1-SP7, 2000 SP1 &SP2	An unchecked buffer overflow vulnerability exists in a subcomponent of FrontPage Server Extensions called the Visual InterDev RAD Remote Deployment Support sub-component, which could let a malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS01-035.asp	Microsoft FrontPage Server Extension Subcomponent Unchecked Buffer Overflow CVE Name: CAN-2001-0341	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[27] ***New variant of vulnerability***[28]	**Windows NT 4.0/2000**	**NetMeeting Version 3.01 (4.4.3385)**	**A security vulnerability exists which could allow a malicious user to temporarily prevent an affected machine from providing any NetMeeting services and possibly consume 100% CPU.** ***A remote Denial of Service vulnerability may be exploited when a malicious client sends a particular malformed string to a port on which the NetMetting service is listening while Remote Desktop Sharing is enabled.***	**Frequently asked questions regarding this vulnerability and the patch can be found at:** **http://www.microsoft.com/technet/security/bulletin/fq00-077.asp**	**Microsoft NetMeeting Desktop Sharing**	**Low**	**Bug discussed in newsgroups and websites. Exploit has been published**
Multiple Vendors[29]	Multiple	ezboard 6.2; Infopop Ultimate Bulletin Board 6.0, 6.0.1-6.0.3; VBulletin 1.0.1 lite, 2.0 rc 2; WWW Threads 5.4	A vulnerability exists in the cgi application, which could let a malicious user supply hostile querystrings concealed within posted image reference.	No workaround or patch available at time of publishing.	Multiple Vendor CGI Script Forced URL Request	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[30]	Multiple	Symbol Technologies Access Point Series 41X1	A vulnerability exists in several 802.11b Access Point devices in that they may reveal the Wired Equivalent Privacy (WEP) key that is associated with the wireless network. This could potentially let a remote malicious user gain unrestricted access.	Symbol Technologies has made a firmware update available. Contact your vendor for information about this update.	Symbol Technologies Firmware Insecure SNMP	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[26] Microsoft Security Bulletin, MS01-035, June 21, 2001.
[27] Microsoft Security Bulletin, MS00-077, October 13, 2000.
[28] Microsoft Security Bulletin, MS00-077 (version 2.0), June 21, 2001.
[29] Bugtraq, June 14, 2001.
[30] Internet Security Systems Security Advisory, ISS-084, June 20, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[31]	Unix	Linux kernel 2.2- 2.4.3	An access validation vulnerability exists in the handling of process-specific 'mem' files, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Linux procfs Stream Redirection to Process Memory	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors[32, 33, 34, 35, 36]	Unix	Eric Raymond Fetchmail 5.0- 5.8.6	A buffer overflow vulnerability exists in the way headers are handled, which could let a malicious user create malicious e-mails that will cause execution of arbitrary code and gain root access.	**Immunix:** http://download.immunix.org/ImmunixOS/ **Debian:** http://security.debian.org/dists/stable/updates/main **Engarde:** http://ftp.ibiblio.org/pub/linux/distributions/engarde/stable/updates/i686/fetchmail-ssl-5.8.7-1.0.2.i686.rpm **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Caldera:** ftp://ftp.caldera.com/pub/updates/eDesktop/2.4/current/RPMS/fetchmail-5.2.0-2.i386.rpm	Fetchmail Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[37, 38, 39, 40, 41, 42]	Unix	Samba 2.0.5-2.2.0	A vulnerability exists in the smb daemon because it does not sufficiently check NetBIOS name input, which could let a malicious user gain elevated privileges.	**Samba:** http://us1.samba.org/samba/ftp/samba-2.2.0a.tar.gz **Immunix:** http://download.immunix.org/ImmunixOS/ **Trustix:** http://www.trustix.net/pub/Trustix/updates/ **Caldera:** ftp://ftp.caldera.com/pub/updates/OpenLinux **RedHat:** ftp://updates.redhat.com/5.2/en/os/ **Debian:** http://security.debian.org/dists/stable/updates/main/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/	Samba Remote Arbitrary File Creation	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[31] Bugtraq, June 27, 2001.
[32] Immunix OS Security, IMNX-2001-70-025-01, June 13, 2001.
[33] Debian Security Advisory, DSA-060-1, June 16, 2001.
[34] EnGarde Secure Linux Security Advisory, ESA-20010620-01, June 20, 2001.
[35] Conectiva Linux Security Announcement, CLA-2001:403, June 19, 2001.
[36] Caldera International, Inc. Security Advisory, CSSA-2001-022.0, June 20, 2001.
[37] Immunix OS Security Advisory, IMNX-2001-70-027-01, June 26, 2001.
[38] Trustix Secure Linux Security Advisory, 2001-0011, June 27, 2001.
[39] Caldera International, Inc. Security Advisory, CSSA-2001-024.0, June 26, 2001.
[40] Red Hat Security Advisory, RHSA-2001:086-06, June 26, 2001.
[41] Debian Security Advisory, DSA-065-1, June 23, 2001.
[42] Conectiva Linux Security Announcement, CLA-2001:405, June 23, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Munica Corporation[43]	Unix	NetSQL 1.0	A buffer overflow vulnerability exists when a long string is sent to port 6500, which could let a remote malicious user execute arbitrary code and gain root access.	No workaround or patch available at time of publishing.	NetSQL Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Netwin Limited[44]	Windows 98/NT 4.0/2000, Unix	SurgeFTP 1.0b, 2.0a	Two vulnerabilities exist: a directory traversal vulnerability, which could let a malicious user gain sensitive information; and a remote Denial of Service vulnerability when attempting to open a directory named for certain MS-DOS devicenames.	Upgrade available at: http://www.netwinsite.com/surgeftp	SurgeFTP Server Information Disclosure and MS-DOS Device Name Denial of Service	Medium	Bug discussed in newsgroups and websites. Exploits have been published.
OpenSSH[45]	Unix	OpenSSH 2.1-2.3, 2.5-2.5.2, 2.9	A vulnerability exists when OpenSSH is used in an environment using PAM, which could let a remote malicious user bypass restrictions enforced by PAM modules.	No workaround or patch available at time of publishing.	OpenSSH PAM Session Evasion	Medium	Bug discussed in newsgroups and websites. No exploit is required.
Oracle Corporation[46]	Windows 2000, Unix	Oracle8 8.1.5, 8.1.6, 8.1.7	A vulnerability exists in the Oracle implementation of the TNS (Transparent Network Substrate) over the Net8 (SQLNet) protocol, which could let a remote malicious user cause a Denial of Service against any service that relies upon the protocol, including the TNS Listener, Oracle Name Service and Oracle Connections Manager.	Patch available at: http://metalink.oracle.com	Oracle 8i SQLNet Denial of Service CVE Name: CAN-2001-498	Low	Bug discussed in newsgroups and websites.
Oracle Corporation[47]	Windows 2000, Unix	Oracle8 8.1.5, 8.1.6, 8.1.7	A buffer overflow vulnerability exists in the TNS Listener, which could let a remote malicious user execute arbitrary code on the database server.	Patch available at: http://metalink.oracle.com	Oracle 8i TNS Listener Buffer Overflow CVE Name: CAN-2001-499	**High**	Bug discussed in newsgroups and websites.
Perception[48]	Windows	LiteServe 1.25	A vulnerability exists when GET requests are made to the webserver with the name of the cgi-bin directory as a MS-DOS name directory, which could let a malicious user gain sensitive information.	Upgrade available at: http://www.cmfperception.com/liteserve.html	LiteServe Script Source Code Disclosure	Medium	Bug discussed in newsgroups and websites. This vulnerability can be exploited with a web browser.

[43] SecurityFocus, June 15, 2001.
[44] Bugtraq, June 19, 2001.
[45] Bugtraq, June 19, 2001.
[46] Network Associates, Inc. COVERT Labs Security Advisory, COVERT-2001-03, June 27, 2001.
[47] Network Associates, Inc. COVERT Labs Security Advisory, COVERT-2001-04, June 27, 2001.
[48] eSecurityOnline Free Vulnerability Alert 3730, June 27, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Ralf S. Engelschall[49]	Unix	ePerl 2.0-2.2.9	An input validation vulnerability exists because the preprocessor allows foreign data to be “safely” included using the ‘sinclude’ directive, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	ePerl Foreign Code Execution	**High**	Bug discussed in newsgroups and websites.
SCO[50]	Unix	UnixWare 7.0	Buffer overflow vulnerabilities exist in the ‘uuxqt,’ ‘uuxcmd,’ ‘uucico,’ ‘bnuconvert,’ ‘uucp,’ and ‘uux’ utilities, which could let a malicious user elevate his/her privileges.	Patch available at: ftp://ftp.sco.com/pub/security/unixware/sr847405/erg711716a.Z	Multiple UnixWare Buffer Overflow Vulnerabilities	Medium	Bug discussed in newsgroups and websites.
Silcon Graphics, Inc.[51]	Unix	Performance Co-Pilot 2.1.1- 2.2	A symbolic link vulnerability exists in the user-definable log directory, ‘pmpost’, which could let a malicious user gain superuser privileges if ‘pmpost’ is setuid root.	Upgrade available at: http://oss.sgi.com/projects/pcp/download/pcp-2.2.1.tar.gz	Performance Co-Pilot pmpost Symbolic Link	**High**	Bug discussed in newsgroups and websites. Exploit script has been published
Sun Micro-systems, Inc.[52]	Unix	Solaris 8.0, 8.0_x86	A buffer overflow vulnerability exists in the way Libsldap handles the ‘LDAP_OPTIONS’ environment variable, which could let a malicious user compromise root.	No workaround or patch available at time of publishing.	Solaris libsldap Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[53]	Unix	SunVTS 4.0-4.3	A buffer overflow vulnerability exists in the ‘ptexec’ command, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Solaris ‘ptexec’ Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Sun Micro-systems, Inc.[54]	Unix	Solaris 8.0	A buffer overflow vulnerability exists in the ‘cb_reset’ command included with the SUNWssp package, which could let a malicious user execute arbitrary code/commands.	No workaround or patch available at time of publishing.	Solaris ‘cb_reset’ Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[49] Bugtraq, June 19, 2001.
[50] Caldera International, Inc. Security Advisory, CSSA-2001-SCO.4, June 27, 2001.
[51] Bugtraq, June 18, 2001.
[52] Bugtraq, June 26, 2001.
[53] Securiteam, June 24, 2001.
[54] Bugtraq, June 20, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Micro-ystems, Inc.[55]	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	A buffer overflow vulnerability exists in the print protocol daemon, 'in.lpd', which could let a remote malicious user execute arbitrary code with super user privilege.	Administrators are advised to either apply network access control to the service or disable 'in.lpd'. The daemon can be disabled by commenting out its associated line in '/etc/inetd.conf' and re-starting inetd. Sun Microsystems has acknowledged this vulnerability; however, the actual patches will not be downloadable until sometime this month.	Solaris Print Protocol Daemon Remote Buffer Overflow CVE Name: CAN-2001-0353	**High**	Bug discussed in newsgroups and websites.
SurfControl[56]	Windows NT 4.0	SuperScout 2.6.1.6, 3.0.1, 3.0.2; CyberPatrol 5.0	A vulnerability exists when a proxy server is used due to the fact that SurfControl cannot handle multiple packets, which could let a malicious user access sensitive information.	No workaround or patch available at time of publishing.	SurfControl Filter Bypass	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Tarantella[57]	Unix	Enterprise 3 3.1	A directory traversal vulnerability exists in ttawebtop.cgi, which could let a remote malicious user view sensitive information.	No workaround or patch available at time of publishing.	Tarantella TTAWebTop. CGI Arbitrary File Viewing	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Trend Micro, Inc.[58]	Windows NT 4.0/2000	InterScan Web Manager 1.2	A buffer overflow vulnerability exists in 'RegGo.dll', which could let a remote malicious user execute arbitrary code.	Trend Micro is aware of this vulnerability and it will reportedly be fixed in the next release of InterScan WebManager.	InterScan WebManager RegGo.dll Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
W3M[59]	Unix	W3M 0.1.10, 0.1.3, 0.1.4, 0.1.6-0.1.9, 0.2, 0.2.1	A buffer overflow vulnerability exists in the 'w3m' client program, which could let a remote malicious user execute arbitrary commands.	A patch to fix this issue was announced on a w3m developer mailing list at: http://mi.med.tohoku.ac.jp/~satodai/w3m-dev/200106.month/2066.htm	W3M Malformed MIME Header Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

[55] Internet Security Systems Security Advisory, ISS-080, June 19, 2001.
[56] Bugtraq, June 18, 2001.
[57] Securiteam, June 28, 2001.
[58] SNS Advisory No.33, June 21, 2001.
[59] SNS Advisory No.32, June 21, 2001.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between June 15 and June 28, 2001, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 12 scripts, programs, and net-news messages containing holes or exploits were identified. *At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script name	Script Description
June 28, 2001	Extremail-exp.c	Script which exploits the eXtremail Remote Format String vulnerability.
June 28, 2001	Ntping_exp.c	Script which exploits the Juergen Schoenwaelder scotty ntping Buffer Overflow vulnerability.
June 27, 2001	**Spew.C**	**Script which exploits the Linux procfs Stream Redirection to Process Memory vulnerability.**
June 21, 2001	Fpse2000ex.C	Script which exploits the MS FrontPage Server Extension Subcomponent Unchecked Buffer Overflow vulnerability.
June 21, 2001	**Killcerb.EXE**	**Exploit for the Cerberus FTP Server Buffer Overflow Denial of Service vulnerability.**
June 21, 2001	**Tradecli.c**	**Script that exploits the Arcadia Internet Store Multiple vulnerability.**
June 18, 2001	Isapi-dos2.c	Script which exploits the MS Index Server and Indexing Service ISAPI Extension Buffer Overflow vulnerability.
June 18, 2001	Pm.C	Script which exploits the SGI Performance Co-Pilot pmpost Symbolic Link vulnerability.
June 18, 2001	**Udirectory.pl**	**Perl script which exploits the Microburst uDirectory Remote Command Execution vulnerability.**
June 17, 2001	**Ghttp.C**	**Script which exploits the Gaztek HTTP Daemon Buffer Overflow vulnerability.**
June 16, 2001	Xrxvt.sh	Script which exploits the Rxvt Buffer Overflow vulnerability.
June 15, 2001	**Netsql-ex.c**	**Script which exploits the NetSQL Remote Buffer Overflow vulnerability.**

Trends

Probes/Scans:

CERT/CC continues to observe increased network reconnaissance activity and a significant increase in the number of generalized port scans of hosts.

Other:

The NIPC and FedCIRC have recently received information on attempts to locate, obtain control of and plant new malicious code known as "W32-Leaves.worm" on computers previously infected with the SubSeven Trojan. For more information, see ADVISORY 01-014, located at: http://www.nipc.gov/warnings/advisories/2001/01-014.htm.

A worm called DoS.Storm.Worm seeks out Microsoft Internet Information Services (IIS) systems that have not applied the proper security patches. Any systems that the worm finds are then infected with the worm. The payload of this worm performs a Denial of Service attack on www.microsoft.com (See Virus Section).

Recent reports on IIS vulnerabilities and the large amount of NT servers being penetrated using different exploits have raised the need to tighten the security of IIS version 5.0 servers. Please see the IIS version 5.0 checklist at: http://www.microsoft.com/technet/security/iis5chk.asp.

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

PE_MARI.A (Aliases: MARI.A, I-Worm.Mari.b, W95.Smoker.Worm@mm) (File Infector): This memory-resident virus propagates via Microsoft Outlook by sending a copy of itself to all addresses listed in an infected user's address book. It arrives in an e-mail with the subject line “Hi!!!” and the attachment SYSTEM32.EXE. When in memory, it displays the icon of a marijuana leaf on the taskbar.

VBS.Chism.A@mm (Visual Basic Script Worm): This is a simple mass-mailing worm. The worm contains several payloads that are executed only on certain days of the month. It also e-mails itself to all contacts in the Microsoft Outlook Address Book.

VBS.LoveLetter.CQ (Visual Basic Script Worm): This is a minor variant of the LoveLetter virus family. This variant does not contain the viral overwriting function found in many of the other variants but it does contain mass-mailing and network-awareness functions. The e-mail arrives in the following format:

Subject: One of this mail
Body: True Story....

Due to an error in the code, no attachment is sent with the e-mails. This limits the worm's ability to spread. The registry is also modified to run the worm when Windows starts. The worm creates the file Mylinong.hta and displays this the first time that the worm is executed. This HTML page contains a note from the author of the script.

VBS/Merlin@MM (Alias: VBS.Merlin.A@mm (NAV) (Visual Basic Script Worm): This is a mass-mailing and file appending VBScript virus which has various date triggering payloads. When run, it creates a registry run key to load itself at startup at:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\

The script then attempts to append .VBS and .VBE files with its code and delete .DOC files. (Note: the virus also appends itself as well. Once this has occurred, it will no longer run). It attempts to copy itself to the WINDOWS directory on all network drives. Five hundred randomly named folders are created on the root of the C drive. Copies of the script are saved to %WinDir%\WindowsXP.html and %WinDir%\%random name%.VBS. An e-mail message is sent to all recipients found in the Outlook address book. The mIRC Internet Relay Chat client SCRIP.INI file is modified to send the %WinDir%\WindowsXP.html file to all users upon joining an IRC channel that an infected user is on. If the day of the week is 2, then the script hides the desktop, attempts to download and run another VBScript, delete the following files, and then exit Windows:

%WinDir%\User.dat

%WinDir%\User.bak
%WinDir%\System.dat
%WinDir%\System.bak
%WinDir%\Regedit.exe

If the day of the week is 4, the script attempts to append the C:\AUTOEXEC.BAT file with this disk formatting command, and then exit Windows: format C: /q /autotest /u. If the day of the week is 5, the script attempts to hide the Windows desktop. If the day of the week is ???, the script attempts to get the Microsoft Agent, Merlin character to speak the text: "Hör nicht auf zu strahlen, kleiner Stern!" Finally, the Windows Registered Owner is set to: Kleiner Stern

W32/Leave-A (Aliases: W32/Leave, W32.Leave.Worm) (Win32 Worm): This is a worm which affects machines already infected with Troj/Sub7 backdoor server program. When the worm is run, it copies itself into the Windows system directory with the filename REGSV.EXE. Depending on the operating system version, the worm creates one of the registry keys:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run
or
HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices

so that REGSV.EXE is run when Windows is started. The worm attempts to find out if the infected computer is online by checking if it can access certain well-known domains such as altavista.com or yahoo.com. If it is successful, the worm attempts to download a few HTML files from Internet sites that were presumably set up by the virus writer. The worm has at least three components: REGSV.EXE, REGISTRY.DLL and BIN.DLL. BIN.DLL is used to infect several programs that are part of the standard Windows installation, such as CALC.EXE or REGEDIT.EXE. REGISTRY.DLL contains an SMTP engine, which could be used for sending e-mail messages.

W95.BlueCorners.2049 (Word 95 Macro Virus): This virus is a fairly simple fast infector. It will infect only Windows 9x computers, and it will fail if run on a Windows NT computer. The virus carries a non-destructive payload that is activated on specific dates. When executed, this virus performs the following actions:

It starts by running the host program in a separate process

Next, it infects all .exe files on the same drive as the virus, and on the C drive (if the virus is located elsewhere)

When it is finished infecting files, this virus checks if the date is one of the following:

- January 1
- February 14
- April 1
- May 4
- October 1
- December 25

If the date matches, it activates its payload routine that animates a number of small blue balls in the four corners of the screen.

W97M.NSI.E (Aliases: W97M.NSI, W97M/Nsi.e) (Word 97 Macro Virus): This is a simple Microsoft Word macro virus that infects Normal.dot and other open documents when an infected document is opened.

WM97/Ded-P (Word 97 Macro Virus): This is a polymorphic Word macro virus that infects Microsoft Word documents.

WM97/Marker-CS (Word 97 Macro Virus): This is a Word macro virus that infects Microsoft Word documents. In the months after June, the virus will attempt to create 999999991 files in the C:\Windows subdirectory. The files are named AAxAA.DOC where *x* is a number between 1 and 999999991.

WM97/Marker-GO (Word 97 Macro Virus): This virus has been reported in the wild. It is a corrupted but viable variant ofWM97/Marker-C. Whenever a document is closed, the virus attempts to FTP user information from Word to the Codebreakers site and appends this information to the bottom of the macro as comments.

WM97/Marker-GP (Word 97 Macro Virus): This virus has been reported in the wild. It is a corrupted but viable variant of WM97/Marker-C. Whenever a document is closed, the virus attempts to FTP user information from Word to the Codebreakers site and appends this information to the bottom of the macro as comments.

WM97/Myna-AS (Word 97 Macro Virus): This is a Word macro virus that infects Microsoft Word documents. The virus checks the system clock on the computer, and if the minute is the same as the day (e.g., it is 14 minutes past the hour on the 14th of the month) then the virus may add 10 pentagons into the active document in random colors and sizes.

WM97/Ramz-A (Word 97 Macro Virus): This is a Word macro virus that infects Microsoft Word documents. The virus code contains some Portuguese text and the phrase "AntiMacro - By Pacheco" which under normal circumstances should not be displayed.

WM97/Thus-EQ (Word 97 Macro Virus): This is a variant of the WM97/Thus-T Word macro virus but has no malicious payload. The virus code contains references to 'Thus_001' and 'Anti-Smyser'. The code also contains text explaining that the virus code was modified to remove the payload.

XM97/Laroux-OD (Excel 97 Macro Virus): This is an Excel spreadsheet virus. This variant of the XM97/Laroux family requires the file PERSONAL.XLS in the XLSTART directory, which it uses to replicate.

Trojans

Trojan Horse programs have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2001-01, and items will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are descriptions of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that their anti-virus software detects. *At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
Backdoor.Acropolis	N/A	CyberNotes-2001-04
Backdoor.Bionet.318	**N/A**	**Current Issue**
Backdoor.Netbus.444051	N/A	CyberNotes-2001-04
Backdoor.NTHack	N/A	CyberNotes-2001-06
Backdoor.Quimera	N/A	CyberNotes-2001-06
Backdoor.SMBRelay	N/A	CyberNotes-2001-10
Backdoor.WLF	N/A	CyberNotes-2001-08
Backdoor-JZ	N/A	CyberNotes-2001-02
Backdoor-QN	**N/A**	**Current Issue**
Backdoor-QO	**N/A**	**Current Issue**
Backdoor-QR	**N/A**	**Current Issue**
BAT.Black	N/A	CyberNotes-2001-11
BAT.Install.Trojan	N/A	CyberNotes-2001-04
BAT.Trojan.DeltreeY	N/A	CyberNotes-2001-07
BAT.Trojan.Tally	N/A	CyberNotes-2001-07
BAT_DELWIN.D	N/A	CyberNotes-2001-05
BAT_EXITWIN.A	N/A	CyberNotes-2001-01
BAT_FORMATC.K	**N/A**	**Current Issue**
BioNet	3.13	CyberNotes-2001-07
BSE Trojan	N/A	CyberNotes-2001-07

Trojan	Version	CyberNotes Issue #
DLer20.PWSTEAL	N/A	CyberNotes-2001-05
DMsetup.IRC.Worm	**N/A**	**Current Issue**
Eurosol	N/A	CyberNotes-2001-10
Fatal Connections	2.0	CyberNotes-2001-09
Flor	N/A	CyberNotes-2001-02
Freddy	beta 3	CyberNotes-2001-09
Gift	1.6.13	CyberNotes-2001-09
Goga	N/A	CyberNotes-2001-12
HardLock.618	N/A	CyberNotes-2001-04
Jammer Killah	1.2	CyberNotes-2001-10
JAVA_STORM.A	**N/A**	**Current Issue**
JS.StartPage	N/A	CyberNotes-2001-07
Noob	4.0	CyberNotes-2001-09
PERL/WSFT-Exploit	N/A	CyberNotes-2001-11
PHP/Sysbat	N/A	CyberNotes-2001-02
PIF_LYS	N/A	CyberNotes-2001-02
PWSteal.Coced240b.Tro	N/A	CyberNotes-2001-04
PWSteal.Trojan.D	**N/A**	**Current Issue**
SadCase.Trojan	N/A	CyberNotes-2001-09
Scarab	1.2c	CyberNotes-2001-10
SennaSpy Generator	**N/A**	**Current Issue**
Troj/Futs	N/A	CyberNotes-2001-07
Troj/Keylog-C	N/A	CyberNotes-2001-08
Troj/KillCMOS-E	N/A	CyberNotes-2001-01
Troj/Unite-C	N/A	CyberNotes-2001-09
TROJ_AOL_EPEX	N/A	CyberNotes-2001-01
TROJ_AOLWAR.B	N/A	CyberNotes-2001-01
TROJ_AOLWAR.C	N/A	CyberNotes-2001-01
TROJ_APS.216576	N/A	CyberNotes-2001-03
TROJ_ASIT	N/A	CyberNotes-2001-07
TROJ_AZPR	N/A	CyberNotes-2001-01
TROJ_BADTRANS.A	N/A	CyberNotes-2001-08
TROJ_BAT2EXEC	N/A	CyberNotes-2001-01
TROJ_BCKDOR.G2.A	N/A	CyberNotes-2001-11
TROJ_BKDOOR.GQ	N/A	CyberNotes-2001-01
TROJ_BUSTERS	N/A	CyberNotes-2001-04
TROJ_CAINABEL151	1.51	CyberNotes-2001-06
TROJ_CHOKE.A	**N/A**	**Current Issue**
TROJ_DARKFTP	N/A	CyberNotes-2001-03
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-04
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-05
TROJ_EUTH.152	N/A	CyberNotes-2001-08
TROJ_FIX.36864	N/A	CyberNotes-2001-03
TROJ_FUNNYFILE.A	N/A	CyberNotes-2001-09
TROJ_GLACE.A	N/A	CyberNotes-2001-01
TROJ_GNUTELMAN.A	N/A	CyberNotes-2001-05
TROJ_GOBLIN.A	N/A	CyberNotes-2001-03
TROJ_GTMINESXF.A	N/A	CyberNotes-2001-02
TROJ_HAVOCORE.A	N/A	CyberNotes-2001-09
TROJ_HERMES	N/A	CyberNotes-2001-03
TROJ_HFN	N/A	CyberNotes-2001-03
TROJ_ICQCRASH	N/A	CyberNotes-2001-02
TROJ_IDENTD.B	N/A	CyberNotes-2001-11
TROJ_IE_XPLOIT.A	N/A	CyberNotes-2001-08
TROJ_IF	N/A	CyberNotes-2001-05
TROJ_INCOMM16A.S	N/A	CyberNotes-2001-09
TROJ_JOINER.15	N/A	CyberNotes-2001-02

Trojan	Version	CyberNotes Issue #
TROJ_JOINER.I	N/A	CyberNotes-2001-08
TROJ_LASTWORD.A	N/A	CyberNotes-2001-09
TROJ_LATINUS.SVR	N/A	CyberNotes-2001-12
TROJ_LEAVE.A	**N/A**	**Current Issue**
TROJ_LINONG.A	**N/A**	**Current Issue**
TROJ_MADBOX.A	**N/A**	**Current Issue**
TROJ_MADBOX.B	**N/A**	**Current Issue**
TROJ_MATCHER.A	N/A	CyberNotes-2001-08
TROJ_MEGA.A	N/A	CyberNotes-2001-12
TROJ_MOONPIE	N/A	CyberNotes-2001-04
TROJ_MOONPIE.A	N/A	CyberNotes-2001-11
TROJ_MSWORLD.A	N/A	CyberNotes-2001-12
TROJ_MTX.A.DLL	N/A	CyberNotes-2001-09
TROJ_MYBABYPIC.A	N/A	CyberNotes-2001-05
TROJ_NAKEDWIFE	N/A	CyberNotes-2001-05
TROJ_NARCISSUS.A	N/A	CyberNotes-2001-09
TROJ_NAVIDAD.E	N/A	CyberNotes-2001-01
TROJ_NEWSFLOOD.A	**N/A**	**Current Issue**
TROJ_PARODY	N/A	CyberNotes-2001-05
TROJ_PICSHOW.A	N/A	CyberNotes-2001-10
TROJ_PORTSCAN	N/A	CyberNotes-2001-03
TROJ_PSW.GINA.A	**N/A**	**Current Issue**
TROJ_Q2001	N/A	CyberNotes-2001-06
TROJ_QZAP.1026	N/A	CyberNotes-2001-01
TROJ_RUNNER.B	N/A	CyberNotes-2001-03
TROJ_RUX.30	N/A	CyberNotes-2001-03
TROJ_SCOUT.A	N/A	CyberNotes-2001-08
TROJ_SUB7.21.E	2.1	CyberNotes-2001-05
TROJ_SUB7.22.D	.22	CyberNotes-2001-06
TROJ_SUB7.401315	N/A	CyberNotes-2001-01
TROJ_SUB7.MUIE	N/A	CyberNotes-2001-01
TROJ_SUB7.V20	2.0	CyberNotes-2001-02
TROJ_SUB722	2.2	CyberNotes-2001-06
TROJ_SUB722_SIN	N/A	CyberNotes-2001-06
TROJ_SUB7DRPR.B	N/A	CyberNotes-2001-01
TROJ_SUB7DRPR.C	N/A	CyberNotes-2001-03
TROJ_TPS	N/A	CyberNotes-2001-05
TROJ_TWEAK	N/A	CyberNotes-2001-02
TROJ_VAMP.A	**N/A**	**Current Issue**
TROJ_VBSWG_2B	N/A	CyberNotes-2001-07
TROJ_WARHOME.A	N/A	CyberNotes-2001-12
TROJ_WEBCRACK	N/A	CyberNotes-2001-02
TROJ_WINMITE.10	N/A	CyberNotes-2001-08
Trojan.MircAbuser	N/A	CyberNotes-2001-04
Trojan.PSW.M2.14	N/A	CyberNotes-2001-07
Trojan.RASDialer	N/A	CyberNotes-2001-06
Trojan.Sheehy	N/A	CyberNotes-2001-05
Trojan.Taliban	N/A	CyberNotes-2001-07
Trojan.W32.FireKill	N/A	CyberNotes-2001-07
Trojan/PokeVB5	N/A	CyberNotes-2001-07
VBS.Cute.A	N/A	CyberNotes-2001-05
VBS.Delete.Trojan	N/A	CyberNotes-2001-04
VBS.Lumorg	N/A	CyberNotes-2001-09
VBS.Over.Trojan	N/A	CyberNotes-2001-10
VBS.Phybre	N/A	CyberNotes-2001-12
VBS.Reset	N/A	CyberNotes-2001-12
VBS.SystemColor.A	N/A	CyberNotes-2001-11
VBS.Trojan.Noob	N/A	CyberNotes-2001-04

Trojan	Version	CyberNotes Issue #
VBS.Zeichen.A	N/A	CyberNotes-2001-08
VBS_HAPTIME.A	N/A	CyberNotes-2001-09
VBS_IESTART.A	N/A	CyberNotes-2001-11
W32.BatmanTroj	N/A	CyberNotes-2001-04
W32.BrainProtect	N/A	CyberNotes-2001-07
Y3K Rat	1.6	CyberNotes-2001-11

Backdoor.Bionet.318: This is a malicious backdoor Trojan. It behaves similar to SubSeven, Netbus, and BackOrifice. The Trojan acts as the server application that allows a remote user to control and retrieve information from an infected computer. Some of the capabilities include searching, retrieving and sending files, stealing passwords, changing the colors and resolution, playing sounds, and changing the date and time. When executed for the first time, this program installs itself into the \Windows\System folder using a configurable name. The following registry key is also added with multiple entries:

HKEY_LOCAL_MACHINE\Software\GCI\BioNet 3

Once the server program is installed, the client program can access the server on a predefined, configurable port. The remote user can be notified that the server application has been installed on the victim's computer. The server can send a page using ICQ, send a notification by IRC, or send an e-mail message. The default server program is packed with UPX, so it may be variable in size, depending on the type and version of packer used. The server is executed upon Windows startup. Either the Windows registry, Win.ini, or System.ini is modified to run the program automatically.

Backdoor-QN (Alias: Backdoor.Belio081 (AVX)): This is a remote access Trojan and IRC Bot. When run, it copies itself to the Windows System directory with a random 8-character name and an .EXE extension. This program then configures the infected system to act as a server and connects to an IRC server. A registry run key is created to run the Trojan at startup:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\servonce=%SysDir%\[Trojan-name.exe]

An additional registry key is created to store various parameters for the Trojan:

HKCU\Software\Microsoft\sds

Backdoor-QO: This is a remote access Trojan program. It is a UPX packed Delphi executable. When run, it acts as an FTP server, opening port 3332 on the local machine. It also creates a registry run key to load the program at startup:

HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Win Name\%TrojanPath%

The IP address of the infected system and the current username is sent to the author of the Trojan via an ICQ page.

Backdoor-QR: This is a remote access and keylogger Trojan. When run, TCP/IP ports 12973 and 12975 are opened to allow an attacker to connect to the infected system. Various system information and keystrokes entered by the local user are stored in a database and are retrievable by an attacker. Several files are used to store this data:

%TrojanPath%\SwCon.BLB
%TrojanPath%\SwCon.DAT
%TrojanPath%\SwCon.IDX
%SysDir%\AddIpa.dll
%SysDir%\Ipopi.dll
%SysDir%\Mcati.dll
%SysDir%\Netcar.dll

The program creates a registry run key to load itself at startup:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\%TrojanFileName%\%TrojanFileName%.EXE

This call will likely fail as the full path is not specified in the registry. Non-malicious DLL files, Imech.dll and WsHk32.dll, are also created and used by the this Trojan:.

BAT_FORMATC.K (Alias: FORMATC.K): Upon execution, this Trojan forces an infected user's computer to connect to itself 20 times using Telnet. It uses port 12345 to connect and then launches Windows Explorer 14 times, after which it formats drive C.

DMsetup.IRC.Worm (Alias: IRC-Worm.DmSetup.C): This is an IRC Trojan worm that sends itself to other users in the IRC channel. It creates the Godicq.ini file in the \Mirc folder. When executed, it performs the following actions:

1. It open a DOS window and prompts the user to "Press any key"
2. When a key is pressed, colorful ovals are displayed until another key is pressed
3. When that key is pressed, the worm displays a message to a DOS window: "START UP ERROR: Can not find vital data!"
4. Next, the worm copies itself as Godicq.exe to the following folders (if they exist):
   C:\
   C:\Windows\
   C:\Mirc\
   C:\Windows\System\
   C:\YOUARENOTSURPOSEDTOBELOOKINGATTHIS\
   C:\Progra~1\
   C:\Dos\
   C:\Quake\
   C:\Doom\
   C:\Doom2\
   C:\Games\
   C:\Pics\
5. The string GODICQ -inauto is added to the C:\Autoexec.bat file to run the worm at startup
6. The next time that Windows starts, the worm creates the Lim.exe file in the same folders in which Godicq.exe was created. It also adds another string, Lim.exe -inauto, to the C:\Autoexec.bat file
7. The worm also creates the following files:
   C:\Mirc\Godicq.ini
   C:\Mirc\Mirc.ini
   C:\Mirc\Lim.ini
   C:\Ni.cfg
8. The C:\Mirc\Mirc.ini file is copied to C:\Mirc\Bakupwrks.ini

The files C:\Mirc\Godicq.ini and C:\Mirc\Lim.ini are the actual IRC worms, and they contain the instructions to send the Godicq.exe or Lim.exe file to other IRC users.

JAVA_STORM.A (Aliases: TROJ_STORM.A, STORM.A, DoS.Storm.Worm, STORM.A): This Trojan worm exploits a vulnerability of Microsoft Internet Information Services (IIS) 4.0 and 5.0 called Web Server Folder Traversal. It opens several ports to allow a remote user access to an infected system. It initiates a Denial of Service attack against www.microsoft.com and sends e-mail to gates@microsoft.com. It installs or uploads a Java Runtime Environment (JRE) in a target system, which it needs in order to function properly. Upon execution, it creates six (6) worker threads that perform the following:

Scan Internet Protocols for IIS vulnerability
Open FTP/Telnet/Console ports for remote access
Denial of Service attack against the Microsoft Web server
Send mass e-mails to the Microsoft Web server

It uses the host IP to scan ten million IPs for IIS vulnerability before its thread terminates. It connects to port 80 and checks whether it can exploit the vulnerability found in IIS and then uses a series of special Unicode characters to allow a remote hacker access to the infected system. When a connection is established, it copies itself to the system and then sends an e-mail to Agberd.Celine@gmx.net using a dummy pop3 account with information identifying an exploited system's IIS. The pop3 account mail server it uses is mail.gmx.net, the username is 8562348, and the password is Java/lang. The worm is copied to the C:\winnt\system32 folder. It uploads and executes a self-extracting ARJ file STORM.EXE, which copies the worm and the JRE files to a "STORM" folder in system32. When a port for remote access is opened in FTP, it opens port 69 for remote access. In Telnet, it opens port 23001 and checks every 50 milliseconds for activity. When a user Telnets to this port, it prompts for a username and password before establishing a connection. To allow access, this worm uses the username “Agberd Celine” and a password “clockdva.” To access a remote console, it opens port 2300 and prompts for a username and password.

For the Denial of Service attack, it sends multiple requests via TCP to the target system and does not respond to the message the target sends so that the target server continues to respond. The attacked server in this case is Microsoft’s http://www.microsoft.com. This worm sends multiple e-mails to gates@microsoft.com with the following text string: “Fuck you!” The sending of e-mails continues unless it is terminated with the “stopbomb” command. Once the worm executes all threads, it modifies the registry with the entry 666 in the Run and RunServices of the following key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion

PWSteal.Trojan.D: This is a Trojan that attempts to steal login names and passwords. These passwords are sent to an anonymous e-mail address. When executed, the PWSteal.Trojan.D performs the following actions:

1. It drops itself into the \Windows\System folder as the Molecule.exe and Molecule.dll files.
2. To enable itself to run at startup, it adds the value: Molecule Molecule.exe /logon to the registry key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
3. It installs hook procedures into a hook chain to monitor the system for any keyboard and mouse messages, which permits the PWSteal.Trojan.D to intercept any keystrokes and any text on the screen.
4. The Trojan drops the intercepted information into a temporary file and sends it out to the virus author’s anonymous e-mail address.

SennaSpy Generator (Alias: Constructor.SennaSpy.2001): This is the Senna Spy Trojan Generator. It allows a user to create variants of the Senna Spy Trojan horse, which are capable of performing malicious actions on the computers of other users.

TROJ_CHOKE.A (Aliases: I-Worm.Choke, W32/Choke, W32/Choke.worm, Win32.Choke, CHOKE, CHOKE.A): This worm propagates via Microsoft’s MSN Messenger. If the infected user does not have MSN installed, the worm will not spread, but will simply copy itself to the root folder where the file was executed and create the file ABOUT.TXT. .

TROJ_LEAVE.A (Aliases: REGSV, REGSV.A, W32/Leave.Worm): This memory-resident backdoor Trojan program causes an infected system to slow down. When opened, it copies itself to a .DLL file in the WINDOWS\SYSTEM directory. It has no other destructive payload.

TROJ_LINONG.A (Alias: VBS_LINONG.A, LINONG): This Trojan spreads via network drives and by e-mail, by sending itself as an attachment to all addresses listed in an infected user’s MAPI address book. It has no destructive payloads, but may perform any or all of the following:

reset the start page of Internet Explorer
display a message
create 600 new folders in an infected user’s Drive C:\ hard drive

TROJ_MADBOX.A (Aliases: Trojan.PSW.Madbox, MADBOX.A): This password stealing, backdoor Trojan is written in Delphi. Once an infected machine is connected to a network, it can send pertinent information on the host to a remote malicious user. Upon execution, this Trojan displays a graphical user interface prompting an infected user to continue activation or cancel running. Once connected, it can transmit some important data from the host victim to a malicious remote user. It does not have a destructive payload and needs to be executed by an infected user to run and activate.

TROJ_MADBOX.B (Aliases: Trojan.PSW.Madbox, MADBOX.B): This is a component of TROJ_MADBOX.A that creates an open port in the infected user's PC and steals information. Upon execution, it checks for an available Internet connection. If a connection exists it attempts to open a random port and wait for the TROJ_MADBOX.A Trojan to connect. The program will immediately exit if TROJ_MADBOX.A is not found. If TROJ_MADBOX.A is connected, it sends the username and password of the infected user's dial-up account, then terminates. This Trojan will open a DOS session and display some garbled text, probably the encrypted username and password.

TROJ_NEWSFLOOD.A (Alias: NEWSFLOOD.A): This Trojan connects to certain newsgroups and posts messages using random e-mail addresses, subject fields, and message bodies with itself as an attachment. It has no destructive payload. Upon execution, it connects to any of the following newsgroups:

alt.test
news.admin.net-abuse.usenet
alt.binaries.nospam.teenfem.nonude
alt.2600
alt.binaries.pictures.erotica.male
alt.religion.scientology
alt.comp.virus
alt.hackers.malicious
alt.religion.Christian
alt.politics.bush
alt.binaries.pictures.asparagus

TROJ_PSW.GINA.A (Aliases: NTHack.dll, PSW.GINA.A, Trojan.PSW.Gina): This is a password-stealing, backdoor Trojan that uses several known Windows NT exploits. It targets Windows NT 4 server and is comprised of components from various sources. Upon infection, a system is vulnerable to unauthorized FTP access, altered network routing configurations, file permissions changes, and excessive bandwidth utilization.

TROJ_VAMP.A (Alias: VAMP.A): This memory-resident Trojan propagates via ICQ. It is generated by TROJ_VAMP.A.GEN. It has no destructive payload. It is written in Visual Basic. Upon execution, it copies itself as SYSMSG332.EXE to the Windows System directory and then creates the following registry entry: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\SYSMSG = "C:\%system directory%\SYSMSG332.EXE. It takes advantage of the "ICQ file extension" exploit. Every 1-20 minutes, it hides the file transfer window while it sends itself to other ICQ users as THIS ROX.ZIP .EXE, which ICQ displays as THIS ROX.ZIP on a target receiver's window.